

1. The first step is to identify the key components of the system. This includes understanding the hardware, software, and data involved.

2. The second step is to define the requirements. This involves determining what the system is intended to do and what it must be able to handle.

3. The third step is to design the system. This includes creating a detailed plan of how the system will be built and how it will be tested.

4. The fourth step is to implement the system. This involves building the system according to the design and testing it to ensure it meets the requirements.

5. The fifth step is to maintain the system. This involves monitoring the system's performance and making any necessary adjustments or updates.

6. The sixth step is to document the system. This involves creating a record of the system's design, implementation, and maintenance.

7. The seventh step is to evaluate the system. This involves assessing the system's performance and determining if it meets the requirements.

8. The eighth step is to improve the system. This involves identifying areas for improvement and making changes to the system.

9. The ninth step is to deploy the system. This involves putting the system into operation and making it available to users.

10. The tenth step is to monitor the system. This involves tracking the system's performance and making any necessary adjustments.

11. The eleventh step is to update the system. This involves making changes to the system to keep it up-to-date.

12. The twelfth step is to retire the system. This involves removing the system from operation and archiving the data.

13. The thirteenth step is to archive the data. This involves storing the data in a secure location for future use.

14. The fourteenth step is to restore the data. This involves recovering the data from the archive in case of a disaster.

15. The fifteenth step is to backup the data. This involves creating a copy of the data to protect it from loss.

16. The sixteenth step is to encrypt the data. This involves converting the data into a secure format to protect it from unauthorized access.

17. The seventeenth step is to authenticate the data. This involves verifying the data's origin and integrity.

18. The eighteenth step is to authorize the data. This involves granting access to the data to authorized users.

19. The nineteenth step is to audit the data. This involves reviewing the data for compliance with regulations.

20. The twentieth step is to report on the data. This involves providing a summary of the data's status and any issues.

John J. Zimmerman

1775

[illegible]

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner

[illegible]